INFORMATION TECHNOLOGY POLICY AND STRATEGY COMMITTEE MINUTES

December 20, 2001
Room 403 State Capitol
9:00-10:00am

<u>In Attendance</u>:

Al Sherwood
Alan Carlsen
Bob Woolley
Brad Brown
Carl R. Meek
Chris Calcut
Chris Heim
Darrus McBride
David Fletcher
David Willis
Douglas Richins
Gary Wixom
Gene Puckett
Greg Gardner
Jeannie Watanabe
Jarrett Taylor
Jim Matsumura
Julie Orchard
Ken Elliott
Kevin Van Ausdal
Kim Thompson
Kim Thorne
Leon Miller
Neal Christensen
Phil Windley
Randy Fisher
Raylene Ireland
Rich North
Rick Gee
Sue Martell

I. Welcome and Approval of Minutes

Phil Windley called the meeting to order at 9:00am. He asked for approval of the May 17th meeting minutes and Leon Miller made the first motion for approval and Rich North made the second motion. Motion passed for approval of the minutes.

II. Executive Order on Information Security (Phil Windley)

The Governor signed the Executive Order on Information Security last week. In summary, the Chief Information Officer shall develop and implement policies promoting the security of State information and information systems. (2) All executive branch agencies shall collaborate in the development of these policies and shall comply with, and cooperate in the implementation of the policies once they are established. (3) ITS under the direction of the CIO shall be responsible for operational implementation of security policies in cooperation with all executive branch agencies.

The goal is to have an enterprise view for security policies because it is difficult to have security policies when you don't take an enterprise approach. The SISC will be the body that executive branch agencies have representation on and can use to collaborate and cooperate in the development of security policies. As you are looking at the things that you are doing, make sure that each agency has a representative serving on SISC and that you are making comments about the security policies that are being developed there.

A question was asked if there would be any significant changes in the way we do security and Phil answered that he didn't think that there would be significant policy changes. For example, most of the things on today's agenda have been in SISC and have been around for a long time and it is just a matter of getting them out there and making sure that everyone knows what they are.

Sue Martell asked if those policies would be brought to ITPSC for more collaboration. Phil said that the collaboration would happen in SISC. Then the policies will be brought to ITPSC for information.

Rich North brought up some concerns he has about the purpose of ITPSC. The statute is pretty clear about the role of this committee and as one of the people who helped draft it he is clear on what the intent was. The ITPSC was set up as a policy approval body. All policies that are proposed by the CIO must come to this committee for approval. The statute is very clear to say that the executive branch should comply with the policy procedures established by the CIO and approved by this body. Rich said that the ITPSC has met two times this year, this being the second time (actually Jan. 18, May 17, & Dec. 20). There have been a significant number of policy proposals, but he's not sure if they have been approved. The public information that is being distributed here is not correct. This committee needs to approve those policies until it is changed by the Legislature for another committee to do the approval process. So in regard to the policies on the agenda today at some point the minutes need to reflect the action taken. Most of the agenda items with the exception of the Privacy Rule require no action. The ITPSC might want to look at the approach on these. The whole purpose was to provide you (Phil) or any CIO with the collective list from the agencies, judicial branch, legislative branch, and education community of their policies that would be a consensus of the executive branch and other entities. There should be action items brought in for debate not just for informational purposes. The public should be notified of the meeting and the minutes should reflect the action items discussed in the meeting. Until the statute changes, the ITPSC cannot change their procedures. Rich will bring a letter this afternoon indicating that the ITPSC fulfill their role until the Governor and CIO bring some legislation that changes that particular relationship. Rich knows that Phil has some proposals to reorganize the process of how ITPSC works and doesn't think we are approving those yet in the Legislature. Until those changes have been made in statute the ITPSC has a statutory duty to fulfill.

Phil Windley responded by saying that if he knew this issue was going to come up he would have invited Gary Doxey to come. The Governor's office position is that the CIO statute has a grant of authority to the ITPSC to create policy which governs the executive branch, but that grant in no way diminishes the Governor's authority to govern the executive branch through executive orders. The Governor still has the right to establish executive orders that govern such matters.

Rich North responded that this was in no way a challenge to the Governor's authority. The Governor certainly has every right to issue executive orders. Executive orders however, do not rise to the level of statute. The Governor has the right to suggest changes for policy and the Legislature is respectful of that and tries to incorporate those in at every opportunity. However, the Legislature has outlined the process under which the CIO's office is to work and until it gets changed executive orders cannot override that.

Phil Windley said that he didn't think that it overrides, but that they are parallel tracks. That is what he understood from talking with Gary Doxey.

Rich North said that he has also talked to Gary Doxey and his concern is that the CIO's office follows the statute as outlined in the code.

Ken Thompson made the comment that at his agency they take the ITPSC packet and very carefully go through it, inquire and give considerable input about what is going to become the policy or at least the direction it will go. When he saw the agenda and saw that most of it was informational, he wanted to know when he would get the chance to give that input or debate the issue.

Another comment was made that his understanding was that the SISC was a subcommittee of ITPSC and they could recommend policy, but ultimately ITPSC would approve the policies.

Phil Windley responded that the executive order only deals with security.

Brad Brown said that it should be reflected in the minutes that the suggestions that may come from SISC would come to ITPSC for discussion and ratification before becoming policy.

Phil Windley said that is an unresolved issue.

Raylene Ireland suggested that we open up the rest of the agenda items to be discussed and debated and then as points are made where they are asking for clarification a presentation could be given at the next meeting.

III. State Information Security Charter &
IV. State Information Security Policy (Bob Woolley)

Most of the issues dealing with security have been voted for in SISC and have been circulated around for 9-10 months with extensive comment. This document represents some minor changes, and Bob would be open to more suggestions or other feedback.

The charter specifically designates responsibility for implementing security policies and security procedures in the state. When this charter was first discussed in SISC, it was a 45-page document that nobody could understand. It was decided to break it down into pieces. The security Executive Order, which was recommended by SISC, is a simple designation of who is on 1st, 2nd, and 3rd base and how this will be accomplished. It incorporates agency responses, which are critical to the process. The specific focus of the charter designates overall responsibilities. The policy is a general document, but within the document it is like a pyramid that will have much more detailed policies. An example is the network access policy. It is very detailed in the policies, but the top level could be for a more general audience rather then technicians. This has been tested and used by the Meta Group and their clients and Gartner has used a similar approach. It is a fairly common approach that has been pretty effective across the United States in terms of actually creating a security policy that people can understand and implement at appropriate levels.

Sue Martell asked if the charter is just an expansion of the security role for ITS with control delegated to the Chief Information Security Officer without additional resources available to implement within ITS. What would you need from the agencies as far as full time employees, level of resources, funds, and length of time for it to be successful?

Bob Woolley responded that they have done several things in ITS to simplify all security functions under one set of management. Previously they were spread all over the place and weren't necessarily talking to one another, as they should. Now they have one person (Rick Gee) in charge of all security in ITS and he reports directly to him (Bob). They already have good working relationships with the security administrators in all of the agencies so; it won't be a big change.

Raylene Ireland asked if this enhanced security role of ITS is going to be absorbed within the organization by the restructuring done in ITS?

Phil Windley responded by saying that he wouldn't look at it as an enhanced security role, just as recognition that as the keeper of the statewide network ITS necessarily has a large role in security and always has. Just as Bob said, the full time employees have just been more spread out. The intention isn't that ITS be involved in all levels of security. However, it is difficult to imagine anything that is strictly an agency security issue unless you have computers that are on their own network that aren't connected to the state network. So, every security issue is a statewide issue.

Bob Woolley said that agencies with those specific concerns should carefully look in the policy at sections 3.1 to 3.7 which are the added sections from UDOT and other agencies that address those issues. If the concerns are not addressed, changes can certainly be made.

Sue Martell asked if the standards in section 3.3 have been established or does that work remain to be completed?

Bob Woolley said that many of the standards are already in place.

Phil Windley said to look at this as a framework that still needs to be flushed out with the larger number of issues.

Sue Martell said that they are being told by another agency (Public Safety) that they must have a certain level of security in order to continue to have access to a system that requires firewalls and encryption. She would like the security information committee to tell them what the standards are and then let them implement them. What would the time frame be? What is the financial impact?

Rick Gee answered that it must be a cooperative effort to build one secure network. What is the lowest common denominator of security that we all need to achieve?

Bob Woolley also said that the cost would depend on implementation constraints. He has an obligation to the state to produce an all-inclusive policy including the most cost efficient procedures where all of the needs and requirements are met. If the agencies leverage each other's resources there won't be a huge financial impact.

Roland Squire said that there are requirements from the FBI as far as access that must be met. They are open to complying to other requirements as long as those first requirements are met.

David Willis raised a concern regarding who has access to data that shouldn't and how to monitor access rights. Reference to section 5.6.

Kevin Van Ausdal pointed out that in the January meeting when this policy was brought to this committee he suggested that the language be softened and was voted down. If a policy is put in place with "musts" that we don't have the full intention of complying with 100% then policy shouldn't say it that way. We are setting ourselves up to be criticized.

Phil Windley asked if there were any more comments or questions on the charter or policy since those two agenda items were blended together.

ACTION ITEM

Raylene Ireland made the motion for the ITPSC to adopt the security policy and security charter and acknowledge the guidelines that accompany them as presented this morning

David Willis said that he was concerned about making a second motion because he feels there needs to be some clarifications made and then presented again before the policy and charter are adopted. Have a sentence on the document that says this is the goal and we will do our best efforts to achieve that.

Phil Windley restated the second motion that the ITPSC adopt the security charter and security policy as a goal to achieve.

Sue Martell then made a substitute to have an effective date as a goal for the agencies to come into compliance. By July 1, 2002.

Ken Elliott said it should be clarified by saying that on July 1, 2002, there should be an internal compliance review and then a report issued that would go to the state security board to check for compliance.

David Willis then said, that by doing this review each agency would understand what the goal is for security and where they are not meeting that goal. If the agency is already measuring itself against the higher standard, it won't be a problem to follow the ITS standards.

Phil Windley responded to a question about security accountability. He said whether we have a policy or not it doesn't matter because if there is a security breech we are all accountable. There are industry standard practices and if we're not in keeping with industry standard practices we are liable for the problems they cause whether there is a policy or not.

Phil Windley then restated the motion to say that to adopt the security charter and security policy as best efforts to achieve with an implementation date of July 1, 2002. Agencies would conduct an internal review and issue a compliance report, financial impact and gap analysis that gives this body (ITPSC) an idea where they sit in respect to meeting these standards. Those reports will be given to Rick Gee in ITS who is the Chief Information Security Officer and he will compile those reports and report back to

ITPSC where there is substantial non-compliance and see what we can do to solve it and what the surrounding issues and risks may be.

The motion was passed.

An amendment was made to the agenda so that Al Sherwood could make it to another meeting. He will go next and will talk about the Privacy Rule.

VIII. Privacy Rule (Al Sherwood)

The privacy rule has been in process for about 6 months. It has gone through a review in the Cabinet and all state agencies and all pieces of input have been accommodated into changes except for one. It was done out of sequence because it went to Administrative Rules before it came to ITPSC for approval. Al asked that on this particular rule, that it be approved as is so it doesn't have a thousand amendments and get held up for another year. The effective date is the 18th.

ACTION ITEM

David Willis made the motion for this rule to be approved as is and the motion was seconded. The motion passed.

V. Network Access Policy (Bob Woolley)

The Network Access Policy was given as an assignment from the prior CIO and is here for comment. There are a lot of people who would like to get access to certain resources on the network and upon what basis can they do that and what are the issues that they need to watch for. Bob would like the ITPSC members to read the document and be prepared at the next meeting to discuss the issues. The document is not ready for action at this meeting.

Rich North asked if this would be a public document out on the Internet.

Phil Windley said that this would not be a citizen-facing document, but that it would drive to some document that may be citizen based. There might be a different statement that says this citizen has access to certain things and be aware you are accessing the State of Utah resources.

Sue Martell said that she has several comments and she will give those directly to Bob Woolley.

Steve Hess had a question asking if wireless and violation of copyright law issues would be included in the 1st paragraph.

Phil Windley would like to see a clear delineation in the Network Access Policy between the things that are about people accessing the network and the issues that concern machines and other networks being connected to the network. They are fundamentally different kinds of issues and can be written about in different ways.

VI. Wireless LAN Standard (Bob Woolley)

This group approved this document some time ago and so this is a significant update that will require additional action at a later date. The main changes to this standard are in the security requirements section. The previous document that was approved didn't have security requirements so it has been fixed with help from SISC. The other thing that has been amended is the contract number references. Look at the security requirement section for comment and just be aware that the contract numbers references have been changed.

Phil Windley recommended that detailed technical notes be made and taken to the SISC meetings so they can be worked into the document.

VII. Production Data Storage Policy (Bob Woolley)

Phil Windley asked Bob to prepare this document for the intent to provide adequate protection to all production data held by agencies across the state. It simply is best practice implementation if agencies already have adequate practices for that then it takes that into cognizance. It is a way to always have a way to get information back. This document is here for comment.

Sue Martell asked for a definition between enterprise resources vs. agency resources. Also, how does this impact our existing systems at Human Services?

Phil Windley answered that the policy states that anything that isn't stored according to these standards would need to have CIO approval. The intention is not to require that you go back and retrofit everything, but that this is applied as we move forward. This will guide our future actions.

Sue Martell asked that a statement be added to the policy clarifying that.

David Willis asked about what kind of data we are storing and what security does it need?

Phil Windley stated that the intent is that we all look at the data we are storing; decide the appropriate level of protection for that data and then do it. There may be data that doesn't merit production level status and in that case this wouldn't apply.

Raylene Ireland wanted to know how long the comment period would be. And it was decided that the deadline would be the next meeting in March.

Brad Brown made the suggestion that the documents need to be marked as drafts.

VIII. State of Utah Email Domain Name Conversion Project (Bob Woolley)

Phil Windley introduced the issue by saying that the Governor has made a strong branding move with agencies towards using *Utah! Where ideas connect.* Part of that branding message is to use *utah.gov* in as many places as possible. Last June-July a system was put in place where employees could register an email address as userid@utah.gov. About 1500 people have already registered. The problem is that system was not intended to handle all 20,000-user ids, but just to get us started. We now have some agencies that are asking all of their employees to use the *utah.gov* as the domain name on their email addresses. In order to accommodate that the email system essentially needs to flip where *utah.gov* is the default domain name and *state.ut.us* is the redirect domain. There were several choices. One choice was to make everyone have the utah.gov email, but then we would have to use unique user ids throughout the entire 25,000-user id space. Another option would be to use the department sub-domain in front of *utah.gov*. For example, instead of *das.state.ut.us* use *das.utah.gov* and both would continue to work.

Bob Woolley suggested that everyone look at the timeline and some specific agency issues and get a feel for it.

Darrus McBride said that the email administrators have looked at it and are okay with how it is presented now. They didn't like the first option, but agreed with the second.

The question was asked if the 1500 people that already have *utah.gov* would have to change to conform to the new proposal. Phil Windley said no and Darrus McBride said that was not what he was told. Phil Windley said it wasn't reasonable to make people change when they have already given out that address.

Rich North says that it is a good idea to centralize the emails. He has spoken with other Legislators and they like the idea, but their immediate concern is that they don't want any changes until after the session ends in March because of the confusion it would cause.

Brad Brown commented that the ITPSC has not discussed and adopted this issue. He feels like he has been caught in a reactionary mode. The train has left the station and he is trying to grab onto it before it is out of sight.

Darrus McBride is concerned with the speed of the implementation.

Phil Windley commented that this should be a smooth transition. If the current system can handle the load for the next three months we should postpone this until after the Legislative session and continue to take comments and then decide the direction we should go. Phil Windley asked that Bob Woolley investigate what it would take to go to a single id and see if that is the direction that we want to go. Employees can continue to register website sub-domain names for *utah.gov.* This is strictly about email.

With the email self-registration there was a glitch in the program that allowed one name to override another employee's same name. Phil Windley asked Bob Woolley to check and make sure that has been fixed.

Brad Brown requested a restate of what has been decided. There is a lot of miscommunication.

ACTION ITEM

Phil Windley restated the motion as a) the intention is to stay the course with the current set up for email addresses and users will continue to register for *utah.gov* email until the issue is revisited at the next ITPSC meeting. b) There is a commitment that names registered at *utah.gov* will continue to work. c) During this period there will be a review done by ITS and state email coordinators and others on what it will take to get us all to a common user id and at the next meeting we will discuss the ramifications of the decision.

Brad Brown made the motion and Raylene Ireland seconded the motion. The motion passed.

IX. Framework for Developing Web Applications (Phil Windley)

A while back Phil Windley promised to provide a framework for state web services and that statewide service would be available for every agency instead of going out and buying their own. This document is the beginning of this process. By the end of the week there should be a contract in place for content management and portal products. We already have an authentication product. This framework is an attempt to bring all of these together and to document, in a detailed way, how those all play together and how you can use them to develop web applications. Ideally when it is finished, you will have a set of documentation that describes the API or web services infrastructure and that anyone developing a web application that is going deployed on this infrastructure will know exactly what they have to do to get single sign on authentication to use the portal and to insure gateway services and this will all be laid out and documented. A companion piece to that is being discussed in the Product Management Council called PATH. The URL is *path.utah.gov*. This is a place where product managers can go and look at all the things they have to do to deploy an e-government product.

This issue is open for comment and review to be given to Bob Woolley.

An exact date and location for the next meeting will be determined later.

Raylene Ireland made the motion to adjourn and Sue Martell seconded the motion.

The meeting was adjourned at 11:30am